CONTRIBUTIONS to SCIENCE, **3**(4):481-491 (2007)
Institut d'Estudis Catalans, Barcelona
DOI: 10.2436/20.7010.01.24 ISSN: 1575-6343 **www.cat-science.cat**

Algorithms and cryptographic protocols using elliptic curves

J. M. Miret*, R. Moreno, J. Pujolàs and M. Valls
Departament de Matemàtica, Escola Politècnica Superior, Universitat de Lleida

Resum

En els darrers anys, la criptografia amb corbes el·líptiques ha adquirit una importància creixent, fins a arribar a formar part en la actualitat de diferents estàndards industrials. Tot i que s'han dissenyat variants amb corbes el·líptiques de criptosistemes clàssics, com el RSA, el seu màxim interès rau en la seva aplicació en criptosistemes basats en el Problema del Logaritme Discret, com els de tipus ElGamal. En aquest cas, els criptosistemes el·líptics garanteixen la mateixa seguretat que els construïts sobre el grup multiplicatiu d'un cos finit primer, però amb longituds de clau molt menor.

Mostrarem, doncs, les bones propietats d'aquests criptosistemes, així com els requeriments bàsics per a que una corba sigui criptogràficament útil, estretament relacionat amb la seva cardinalitat. Revisarem alguns mètodes que permetin descartar corbes no criptogràficament útils, així com altres que permetin obtenir corbes bones a partir d'una de donada. Finalment, descriurem algunes aplicacions, com són el seu ús en Targes Intel·ligents i sistemes RFID, per concloure amb alguns avenços recents en aquest camp.

Paraules clau: corbes el·líptiques, criptosistemes, algoritmes criptogràfics

Abstract

The relevance of elliptic curve cryptography has grown in recent years, and today represents a cornerstone in many industrial standards. Although elliptic curve variants of classical cryptosystems such as RSA exist, the full potential of elliptic curve cryptography is displayed in cryptosystems based on the Discrete Logarithm Problem, such as ElGamal. For these, elliptic curve cryptosystems guarantee the same security levels as their finite field analogues, with the additional advantage of using significantly smaller key sizes.

In this report we show the positive properties of elliptic curve cryptosystems, and the requirements a curve must meet to be useful in this context, closely related to the number of points. We survey methods to discard cryptographically uninteresting curves as well as methods to obtain other useful curves from a given one. We then describe some real world applications such as Smart Cards and RFID systems and conclude with a snapshot of recent developments in the field.

Keywords: elliptic curve, cryptosystems, cryptographic algorithms

1 Introduction

The extended use of computer networks for information transmission and management, as well as the fact that the number of IT-users is increasing day by day, requires the role of security mechanisms to guarantee privacy, integrity or authentication of information. Such needs have been covered using several cryptographic protocols, which often combine symmetric and asymmetric cryptosystems.

One of the major disadvantages of symmetric cryptosystems lies in the key agreement procedure, since users who want to communicate confidentially in the future need to agree on a common secret key using a secure communication channel (in practice, this means they have to meet face to face). Obviously, this is an insurmountable drawback in our digital global era. To overcome this obstacle, Diffie and Hellman [17] suggested in 1976 a secure key agreement protocol that can be performed over insecure communication channels. This proposal is considered the first step towards public key cryptography, where secretly shared information between parties is no longer needed to be confidentially provided. The security of these cryptosystems lies in the hardness of some underlying mathematical problem which is believed to be computationally difficult. Hence, attackers are prevented from obtaining the secret keys from the public ones.

There are two widely used public key cryptosystems. The first is RSA, proposed by Rivest, Shamir and Adleman [67], and

*Author for correpondence: Josep M. Miret. Departament de Matemàtica, Escola Politècnica Superior, Universitat de Lleida. C/ Jaume II, 69, E-25001 Lleida, Catalonia, EU. Tel.: 34 973 702 776. Fax: 34 973 702 716.
Email: miret@matematica.udl.cat

is related to the intractability of the integer factorization problem, namely the inversion of Euler's Totient function. The second is ElGamal cryptosystem [19], whose security lies in the difficulty of the discrete logarithm problem over the multiplicative group of a finite field. In view of the late improvements on factorization algorithms (Lenstra's elliptic curve algorithm and the number field sieve for example) and on those algorithms aimed to solve the discrete logarithm problem (specially Index-Calculus methods), the need for an enlargement in length of the keys is a sensible issue for guaranteeing security.

In this situation, the use of elliptic curves in the design of cryptosystems is a good alternative, since they provide both a reduction in the key lengths while maintaining the same security, and a wider range of choice for the system's parameters (while a change of curve does not necessarily mean a change in the basic arithmetic). Technological industry is already implementing these systems in the development of smart card authentication and telecommunication protocols.

This report provides an overview of the techniques involved in elliptic curve cryptography (ECC), focusing on the needs and problems to be taken into account. We first introduce the notion of an elliptic curve, and we emphasize elliptic curves over finite fields. Then we review some elliptic curve crytosystems and digital signature protocols, such as ECDSA. We then refer to the problem of generating cryptographically good elliptic curves, which is related to the problem of computing their cardinality. The next section is devoted to the usage of ECC in restricted environments such as smart cards and RFID systems. Likewise, some recent research on the cooperative relationship between cryptography and algebraic curves is highlighted. Finally, in the last part of our report we overview some applications such as primality test and factorization algorithms and sketch some topics of current research.

2 Elliptic curves

An elliptic curve over a field $\mathbb{K}$ is an algebraic curve with no singular points, given by an equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \quad a_i \in \mathbb{K},$$

called general Weierstrass equation (see [73]).

Whenever the field characteristic is different from 2 or 3, this equation can be transformed into the reduced Weierstrass form

$$y^2 = x^3 + ax + b, \quad a, b \in \mathbb{K}, \tag{1}$$

with nonzero discriminant $4a^3 + 27b^2 \neq 0$ to avoid singularities.

Then, given an elliptic curve $E/\mathbb{K}$ over a field $\mathbb{K}$, we denote by $E(\mathbb{K})$ the set of points $P = (x, y) \in \mathbb{K} \times \mathbb{K}$ which satisfy the curve equation, along with the infinity point $\mathcal{O}$.

2.1 Group law

An addition operation is defined over $E/\mathbb{K}$ using the chord-tangent method (see Figure 1). It consists of considering the line through two points P and Q (or the tangent line, in case we want to double P). The intersection point of such a line with the elliptic curve is a rational point R. Then the addition point $P+Q$ is obtained taking the symmetric point of R with respect to the x-axis. This operation, called elliptic addition, endows the set $E(\mathbb{K})$ with an abelian group structure, where $\mathcal{O}$ is the identity element.

Analytically, given a curve with equation (1), the coordinates of $P + Q = (x_3, y_3)$, when $P + Q \neq \mathcal{O}$, are obtained in terms of the coordinates of $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ as follows

$$x_3 = \lambda^2 - x_1 - x_2, \quad y_3 = (x_1 - x_3)\lambda - y_1, \tag{2}$$

where $\lambda = (y_1 - y_2)/(x_1 - x_2)$ if $x_1 \neq x_2$, and $\lambda = (3x_1^2 + a)/2y_1$ when $x_1 = x_2$ and $y_1 \neq 0$. The symmetric point of $P = (x, y)$ is $-P = (x, -y)$.

Considering this group law, the scalar multiplication operation is defined as $k \cdot P = P + \overset{k}{\cdots} + P$, for any $P \in E(\mathbb{K})$ and k a natural number. Such an operation, analogous to the exponentiation in multiplicative abelian groups, is important for the elliptic curve cryptography. There exist several algorithms to perform such an operation (see [6]), although the most extended is the binary method, also called double-and-add algorithm (an analogue of the square-and-multiply algorithm in multiplicative abelian groups). This method exploits the binary expression of k, and reduces an exponentiation to a chain of $\log_2(k)$ doublings and additions of points. For instance, $13 \cdot P = \left(2^2(2+1)+1\right) \cdot P = 2\left(2 \cdot P + P\right) + P$. From the point of view of computational complexity, the addition of two different points involves the computation of one inverse and 3 multiplications in the field, while doubling requires one inversion and 4 multiplications.

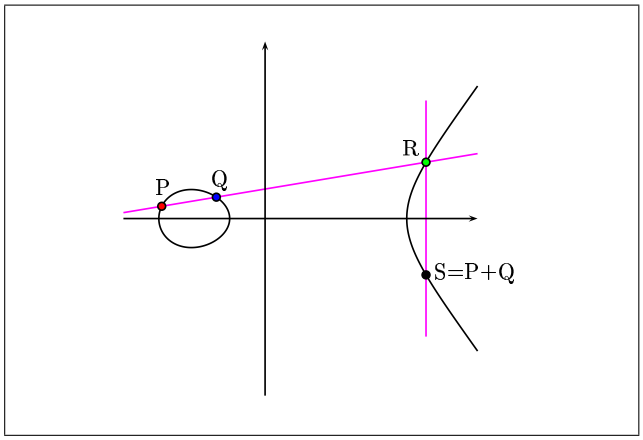

Figure 1. Point addition on elliptic curves over $\mathbb{R}$.

2.2 Elliptic curves over finite fields

From a cryptographic perspective, elliptic curves over finite fields $\mathbb{F}_q$, with $q = p^m$ and p prime, are interesting because they provide instances of finite groups where the discrete logarithm problem is hard. In practice, the most common fields are $\mathbb{F}_p$ or $\mathbb{F}_{2^m}$, where p and m are large enough to grant the desired level of security.

One should stress that the interest on these curves is connected to their number of points. The knowledge of the properties of such a cardinal, as well as the group structure, is crucial in the design of cryptographic applications, and it becomes an important requirement to be taken into account for the development of new schemes and techniques.

Let $\#E(\mathbb{F}_q)$ denote the cardinal of the group of points. It is a well known fact that $\#E(\mathbb{F}_q)$ can be written as $\#E(\mathbb{F}_q) = q + 1 - t$, with t the trace of the Frobenius endomorphism $\varphi : E(\overline{\mathbb{F}_q}) \to E(\overline{\mathbb{F}_q})$, which assigns to each point (x, y) the point (x^q, y^q). Hasse provided [36] a threshold for the value of the trace, and hence for the cardinal of the curve.

Theorem 1 (Hasse) *The trace of the Frobenius endomorphism of a curve $E/\mathbb{F}_q$ satisfies $|t| \leq 2\sqrt{q}$. Consequently, the cardinal of $E(\mathbb{F}_q)$ belongs to the interval $[q + 1 - 2\sqrt{q}, q + 1 + 2\sqrt{q}]$.*

As an example, we can consider the curve $E : y^2 = x^3 + 1013x + 2007$ over the field $\mathbb{F}_p$ with $p = 314159265359$, which has cardinal

$$\#E(F_p) = 31415893030968 = 2^3 \cdot 3 \cdot 13089955457.$$

To obtain points $P = (x, y)$ on the curve, one can take random values x in $\mathbb{F}_p$, checking whether the Legendre symbol of $x^3 + 1013x + 2007$ over p is 1. Hence, there exist two roots y, which correspond to the ordinates of two points with abscissa x, opposite one another. For instance, the points $P = (63510465893, 141411081955)$ and $-P = (63510465893, 172748183404)$ lie on the curve above and their order is 13089955457, since $13089955457 \cdot P = \mathcal{O}$.

The following result after J. W. Cassels [8], and completed by Schoof [72], describes the structure of the group of points of an elliptic curve over a finite field.

Theorem 2 (Cassels) *The group $E(\mathbb{F}_q)$ is isomorphic either to the cyclic group $\mathbb{Z}_m$, where $m = \#E(\mathbb{F}_q)$, or to the group $\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2}$, where $m_1 \cdot m_2 = m$, $m_2 | m_1$ and $m_2 | (q - 1)$.*

Moreover, as J. E. Cremona pointed out in a remark in the Number Theory distribution list [12], the value of m_2 is completely determined by the value of m_1, unless q is one of the integers

$$3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 43, 61, 73, 181, 331,$$

$$547, 4, 9, 27, 81, 25, 49, 121, 841.$$

Hence, in the other cases the cardinal and structure of the group of points is completely determined by a point of order m_1.

On the other hand, E. Waterhouse [47, 78] showed that for any finite field $\mathbb{F}_p$, there exist elliptic curves with cardinal equal to any of the integers in the Hasse interval, and one finds elliptic curves with every possible group structure [69, 77]. This is one of the main advantages provided by elliptic curves: for a given finite field $\mathbb{F}_p$ there is a wide range of cryptographically interesting cardinals, which go through a large interval of length $4\sqrt{p}$.

2.3 Elliptic curves over rings

Elliptic curves defined over rings $\mathbb{Z}_n$, with $n = p \cdot q$ the product of two primes p, q, are also useful in the design of cryptosystems based on the intractability of the integer factorization problem. In fact, the chord and tangent addition law can be extended for points in a curve E over $\mathbb{Z}_n$. However, since there are elements in $\mathbb{Z}_n$ which are not invertible, the addition law is not always well-defined when using analytical expressions like (2).

One way to overcome this is to consider elliptic curves defined on the projective plane $\mathbb{P}^2(\mathbb{Z}_n)$. In this way, the points in the curve are given as triples $[x, y, z]$ satisfying the equation $y^2 z = x^3 + axz^2 + bz^3$ in $\mathbb{Z}_n$. Note that besides point at infinity $[0, 1, 0]$ and the points $[x, y, 1]$ in the affine plane, our curve also contains semi-infinite points $[x, y, z]$ such that $\gcd(z, n)$ is either p or q.

By the Chinese Remainder Theorem, it follows that the mapping $E(\mathbb{Z}_n) \to E(\mathbb{F}_p) \times E(\mathbb{F}_q)$, defined by the natural projections is a bijection, and this endows $E(\mathbb{Z}_n)$ with a group structure compatible with the elliptic addition defined by the chord-tangent method. Moreover, considering $m_p = \#E(\mathbb{F}_p)$ and $m_q = \#E(\mathbb{F}_q)$ it follows that

$$(1 + k \cdot m_p \cdot m_q) \cdot P = P, \quad \forall P \in E(\mathbb{Z}_n), \quad \forall k \in \mathbb{Z}.$$

Similarly, the set of points $E(\mathbb{Z}_{n^2})$ is given a group structure which takes care of the existence of more points at infinity, namely all those with coordinates $\mathcal{O}_k = [k \cdot n, 1, 0]$, $0 \leq k < n$.

3 Elliptic curve cryptosystems

Koblitz [38] and Miller [51] suggested in 1985 to use elliptic curves over finite fields for the design of cryptosystems [6, 33, 47]. Since then, several schemes have been proposed, and at the moment some of them are present in industrial standards (for instance [60]), and some receive the same attention as the most widely used cryptosystems.

The security of most of these schemes relies on the intractability of the discrete logarithm problem in the group of points of an elliptic curve. There also exist proposals concerning curves over the rings $\mathbb{Z}_n$ or $\mathbb{Z}_{n^2}$, $n = p \cdot q$, which base their security on the complexity of the factorization problem. Some of these schemes extend the capabilities of RSA [67], and provide efficient mechanisms for semantically secure cryptography [32].

3.1 ElGamal-type cryptosystems

The cryptosystem introduced by ElGamal [19] in 1985 bases its security on the intractability of the discrete logarithm problem (DLP):

> *Given a cyclic finite group G, a generator g and an element g' in G, find an integer n such that $g' = g^n$, that is, find the discrete logarithm of g' in base g.*

Note that, given g and n, it is straightforward to compute $g' = g^n$. But, the other way round, given g and g', it is generally difficult to compute n. In the particular case that G is the group of points of an elliptic curve over a finite field, it is customary to give this problem the name ECDLP. Elliptic curves are usually taken over finite fields $\mathbb{F}_q$, with $q = p$ or $q = 2^m$.

If one considers ElGamal cryptosystem over the multiplicative group $\mathbb{F}_p^*$ (as in [19]), p should be large enough to grant security. In practice, p is taken such that $p - 1$ has a large prime factor. Otherwise, an attacker could take advantage of the Pohlig-Hellman method [63], which reduces the attack to the DLP over groups whose orders are factors of $p - 1$.

The complexity of the general purpose algorithms which try to solve the DLP (baby step – giant step, Pollard-ρ, Pohlig-Hellman,...) is exponential. However, for the particular case of DLP over $\mathbb{F}_p^*$, there exists a more efficient algorithm, known as the *Index-Calculus* attack [74], which has a subexponential cost.

Table 1. NIST guidelines for public key sizes

DLP& RSA (bits)	ECDLP (bits)	Ratio key sizes	AES (bits)
1024	163	1:6	
3072	256	1:12	128
7680	384	1:20	192
15360	512	1:30	256

The advantage of the ElGamal cryptosystem over the group of points of an elliptic curve lies in the fact that the best-known algorithm to solve ECDLP has exponential cost, hence the size of the group and the keys are allowed to be significantly smaller while offering same security. Table 1 compares the key lengths for a given security level between DLP, ECDLP and the key lengths of the standard symmetric encryption scheme AES [13].

The setup of the cryptosystem consists in taking a prime p which defines the field $\mathbb{F}_p$, two parameters a and b corresponding to an elliptic curve E over $\mathbb{F}_p$, and a point P in E with order n. The cyclic group to consider is the subgroup of $E_{a,b}(\mathbb{F}_p)$ generated by P. With these elements fixed, the secret key is a random integer d in $[1, n-1]$, while the public key is the point $Q = d \cdot P$ in the curve.

The encryption and decryption algorithms work as follows [35, 49]:

Algorithm (ElGamal elliptic curve cryptosystem encryption)
INPUT: The parameters (p, a, b, P, n), the public key Q and the plaintext m.
OUTPUT: The cyphertext $(\alpha_1, \alpha_2, \gamma)$.

- Select a random integer r in $[1, n-1]$.
- Compute the points $r \cdot P = (\alpha_1, \alpha_2)$ and $r \cdot Q = (\beta_1, \beta_2)$ on $E_{a,b}(\mathbb{F}_p)$.
- Compute $\gamma = m \cdot \beta_1$ in $\mathbb{F}_p$.
- Return $(\alpha_1, \alpha_2, \gamma)$.

Algorithm (ElGamal elliptic curve cryptosystem decryption)
INPUT: The parameters (p, a, b, P, n), the private key d and the cyphertext $(\alpha_1, \alpha_2, \gamma)$.
OUTPUT: The plaintext m.

- Compute the point $d \cdot (\alpha_1, \alpha_2) = d \cdot r \cdot P = r \cdot Q = (\beta_1, \beta_2)$ on $E_{a,b}(\mathbb{F}_p)$.
- Obtain the plaintext $m = \gamma \cdot \beta_1^{-1}$ in $\mathbb{F}_p$.
- Return m.

There are still some challenges related to the setup of the elliptic curve cryptosystem, such as computing the cardinal of an elliptic curve, the design of efficient algorithms to obtain cryptographically good elliptic curves (neither non-supersingular nor anomalous) with almost prime cardinal, or finding points whose order is as large as possible. Any improvement in these directions would result in a more efficient setup of the system.

3.2 RSA-type cryptosystems

Koyama, Maurer, Okamoto and Vanstone [41] proposed the so called KMOV cryptosystem using elliptic curves defined over $\mathbb{Z}_n$, $n = p \cdot q$, with p, q two secret primes. The security of the KMOV cryptosystem relies on the hardness of finding the prime factors of n.

The setup of this cryptosystem simply requires two primes p, q such that $p, q \equiv 2 \pmod{n}$. The chosen elliptic curves are defined by an equation $y^2 = x^3 + b$ over $\mathbb{Z}_n$. These curves have $p+1$ points over $\mathbb{F}_p$ and $q+1$ points over $\mathbb{F}_q$. The public key is the pair (n, e), where e is an integer coprime to $(p+1)(q+1)$. The private key is the integer $d := e^{-1}$ modulo $(p+1)(q+1)$. Encryption and decryption work as follows:

Algorithm (KMOV Encryption)
INPUT: The Public Key (n, e) and the plaintext message m.
OUTPUT: The cyphertext (c_1, c_2).

- Represent the message m as a point $M = (m_1, m_2) \in \mathbb{Z}_n \times \mathbb{Z}_n$.
- Take the curve $E : y^2 = x^3 + b$ with $b = m_2^2 - m_1^3 \pmod{n}$.
- Compute the point $e \cdot M = (c_1, c_2)$ on $E(\mathbb{Z}_n)$.
- Return (c_1, c_2).

Algorithm (KMOV Decryption)
INPUT: The private key (p, q, d) and the cyphertext (c_1, c_2).
OUTPUT: The plaintext (m_1, m_2).

- Take the curve $E : y^2 = x^3 + b$ with $b = c_2^2 - c_1^3 \pmod{n}$.
- Compute the point $d \cdot (c_1, c_2) = d \cdot (e \cdot M) = (1 + k(p+1)(q+1)) \cdot M = (m_1, m_2)$ on $E(\mathbb{Z}_n)$.
- Return (m_1, m_2).

Breaking the cryptosystem above is computationally equivalent to breaking RSA. However, the encryption step in KMOV is clearly slower than in RSA.

Because of this, some proposals like Demytko's [15] have appeared. In [15] some of the limitations of KMOV are overcome. For example the curve in the scheme setup is fixed, and there is no restriction on the type of elliptic curves considered. In Demytko's scheme the message is represented as the abscissa of a point on the curve, and in the decryption algorithm one previously needs to know which of the twists of the curve over $\mathbb{F}_p$ and $\mathbb{F}_q$ is being used for the operations — a twist of a curve $E/\mathbb{F}_p : y^2 = x^3 + ax + b$ is given by $E'/\mathbb{F}_p : sy^2 = x^3 + ax + b$ where s is a non-quadratic-residue in $\mathbb{F}_p$, and satisfies $\#E'(\mathbb{F}_p) = p + 1 + t$ if $\#E(\mathbb{F}_p) = p + 1 - t$.

Meyer and Müller [50] proposed another RSA-like cryptosystem using elliptic curves over $\mathbb{Z}_n$. They use a 2-exponent encryption, and breaking it is provably as hard as factoring n. However, Joye and Quisquater [37] prove that Meyer and Müller's scheme is reducible to the Rabin-Williams scheme [79], which relies on the difficulty of extracting square roots modulo a composite integer n.

More recently, Paillier [61] designed a cryptosystem over the ring $\mathbb{Z}_{n^2}$, $n = p \cdot q$, based on the problem of *composite residuosity*:

> *Let n be an integer of the RSA-modulus type, let $g \in \mathbb{Z}_{n^2}^*$ of order a multiple of n and let $\omega \in \mathbb{Z}_{n^2}^*$. The problem is to find an integer m such that there exists $r \in \mathbb{Z}_n^*$ with $\omega = r^n g^m \pmod{n^2}$ (note that under the above assumptions the map $\varepsilon_g : \mathbb{Z}_n^* \times \mathbb{Z}_n \to \mathbb{Z}_{n^2}^*$ which assigns to a pair (r, m) the integer $r^n g^m \pmod{n^2}$ is a bijection).*

The elliptic curve version of Paillier's scheme that we now describe was given by S. Galbraith in [23]. For the setup he considers an integer $n = p \cdot q$ product of two primes p, q, and a curve $E_{a,b}$ over the ring $\mathbb{Z}_{n^2}$. The knowledge of the number of points of $E_{a,b}$ over $\mathbb{F}_p$ and $\mathbb{F}_q$ is a requirement for constructing the private key $d = \text{lcm}(\#E_{a,b}(\mathbb{F}_p), \#E_{a,b}(\mathbb{F}_q))$. The public key is a point Q of $\#E_{a,b}(\mathbb{Z}_{n^2})$ such that $d \cdot Q = [0, 1, 0]$ (for instance, taking a random point Q' and computing $Q = n \cdot Q'$). The encryption and decryption algorithms work as follows:

Algorithm (Paillier-Galbraith Encryption)

INPUT: Parameters (n, a, b), the public key Q and the plaintext m.
OUTPUT: The cyphertext C.

- Represent m as a point $P_m = [m \cdot n, 1, 0]$ of $E_{a,b}(\mathbb{Z}_{n^2})$.
- Choose a random integer $r \in \mathbb{Z}_n$.
- Compute the point $C = r \cdot Q + P_m$ on $E_{a,b}(\mathbb{Z}_{n^2})$.
- Return C.

Algorithm (Paillier-Galbraith Decryption)

INPUT: Parameters (n, a, b), the private key d and the cyphertext C.
OUTPUT: The plaintext m.

- Compute the point $d \cdot C = d \cdot (r \cdot Q + P_m) = d \cdot P_m = [d \cdot m \cdot n, 1, 0]$ on $E_{a,b}(\mathbb{Z}_{n^2})$.
- Obtain the first coordinate $x = d \cdot m \cdot n$ of the point $d \cdot C$.
- Compute $y = x/n$ in $\mathbb{Z}$ and the product $m = y \cdot d^{-1}$ in $\mathbb{Z}_n$.
- Return m.

Despite being efficient, the elliptic curve variant above is not semantically secure [32]: given two plaintexts and the cyphertext of one of them, an adversary may decide in polynomial time which plaintext corresponds to the cyphertext with probability significantly greater than $\frac{1}{2}$. In this direction, Galindo, Martín, Morillo, Takagi and Villar [28, 29] designed a semantically secure cryptosystem that generalizes Paillier-Galbraith's scheme using KMOV-type elliptic curves.

4 Digital signatures using elliptic curves

The electronic communications era in a broad sense, and specially e-commerce, motivate the need for some mechanism for the sender to grant the claimed identity when a receiver obtains his message (*non-repudiation* mechanisms).

Digital signatures (see [18, 22, 66]) emerge as an analogue to manual signatures in ordinary mail. In order to grant the length of the digital signature to be smaller than the message to sign, *hash* functions are used. These functions build in a reproducible way a fixed size *fingerprint* of the message and they are collision resistant. The digital signature depends then on the hashed message and the private key of the signer. As a result, any entity may check the veracity of a signature from the public key of the signer.

The Digital Signature Algorithm (DSA in short) is a variant of the ElGamal signature, which is in its turn the basis of the Digital Signature Standard (DSS). The Elliptic Curve Digital Signature Algorithm (ECDSA) is the elliptic curve analogous to DSA. In fact, this algorithm has been included as a component of the set of cryptographic algorithms Suite B [59] promulgated by the National Security Agency.

The signature generation and verification procedures [35] are as follows (N.B. one uses the same setup parameters as in ElGamal):

Algorithm (ECDSA digital signature generation)

INPUT: The parameters (p, a, b, P, n), the public key Q, the private key d and the plaintext m.
OUTPUT: The message m with the signature (r, s).

- Compute the Hash $h = H(m)$ of the message.
- Choose a random integer k in $[1, n-1]$.
- Compute the point $k \cdot P = (x, y)$ on $E_{a,b}(\mathbb{F}_p)$.
- Compute $r = x \mod n$ (restart if $r = 0$).
- Compute $s = k^{-1}(h + d \cdot r) \mod n$ (restart if $s = 0$).
- Return m and (r, s).

To verify the signature from the Hash of the message one needs to compute the inverse w of s modulo n. Then it is enough to use the public key to compute the point $R = (w \cdot h) \cdot P + (w \cdot r) \cdot Q$ and check that the abscissas of the points R and $k \cdot P$ coincide, because $k = w \cdot h + w \cdot d \cdot r$ and $Q = d \cdot P$.

5 Cryptographically useful elliptic curves

Cryptosystems and digital signature schemes using elliptic curves demand some requirements for the setup, notably the order of the elliptic curves involved must satisfy certain good conditions. Following the cryptographic standard recommendations [60], it should be verified that the group order of $E(\mathbb{F}_p)$ be of the form $f \cdot q$, with q prime and f a *small* integer [39]. Otherwise the curve is vulnerable to the Pohlig-Hellman attack.

It is also convenient that the curve be neither *non-supersingular* nor *anomalous*. Supersingular curves are those with cardinal $p + 1$, and for them the MOV attack [48] transfers

the ECDLP in $E(\mathbb{F}_p)$ to the DLP in $\mathbb{F}^*_{p^k}$, with $k \leq 6$. Anomalous curves are those with cardinal p and, although they resist the MOV attack, there exists a polynomial algorithm which solves the DLP over their group of points.

Hence, it seems reasonable to compute first the cardinal of the curves and check whether this number satisfies the required conditions before using them in cryptographic protocols. Even though the point-counting problem for elliptic curves over $\mathbb{F}_p$ is solved by the well-known Schoof algorithm [71], with polynomial complexity $\mathrm{O}(\log^8 p)$, its practical implementation turns out to be unfeasible when p is large.

The basic idea of the Schoof algorithm is the computation of the trace t of the Frobenius endomorphism of the curve $E/\mathbb{F}_p$ modulo different suitably chosen small primes ℓ such that $\prod \ell > 4\sqrt{p}$. The value of t is recovered with the Chinese Remainder Theorem, and from t the cardinal $\#E(\mathbb{F}_p) = p + 1 - t$ is obtained. The contributions given by Atkin and Elkies (see [6]) allow a factor of degree $(\ell - 1)/2$ of the ℓ-division polynomial of the curve to be found. This is used to improve the implementation of the initial algorithm of Schoof, and all together constitute the so called SEA algorithm.

Later, Fouquet and Morain [20] extend the moduli ℓ in the SEA algorithm to prime powers ℓ^s. They propose to compute the values s from the graph of volcanoes of ℓ-isogenies.

In another direction, the algorithm of Satoh [70] provides the computation of the cardinal of elliptic curves over $\mathbb{F}_{2^m}$ for large values of m (see the communications of Harley and Lercier [44] in the Number Theory distribution list).

5.1 Algorithms to discriminate non-useful elliptic curves

Elliptic curves where DLP is easy to solve are not useful for cryptographic applications. The DLP in elliptic curves with cardinal equal to a product of small primes is solvable using the Pohlig-Hellman method. Therefore high powers of primes are not desirable in cardinals of interesting curves.

In [53] a polynomial algorithm is given to determine the 2-Sylow subgroup of an elliptic curve E over a finite field $\mathbb{F}_p$. For small primes $\ell \neq 2$, this procedure can be generalized to obtain the ℓ-Sylow subgroups of $E(\mathbb{F}_p)$ [57]. The summary of the steps is as follows.

- Compute the rational points of order ℓ of the curve from the ℓ-division polynomial.
- Assuming the existence of a point P of order ℓ^n such that $\ell \cdot Q = P$, find, whenever it exists, a point Q of order ℓ^{n+1}. For short, one says that Q is an ℓ-divisor point of P.

An iteration of the process above allows a point to be obtained whose order is the maximal ℓ-power. At each step, a suitable ℓ-divisor point is obtained with the roots of two degree ℓ polynomials with coefficients in the ground field. To obtain these coefficients, a generalization of Vélu's formulae for isogenies between elliptic curves is introduced [52].

The output of the algorithm is a pair of integers (n, r), $0 \leq r \leq n$, where n is the largest integer such that points of order ℓ^n exist and r is the integer such that the ℓ-Sylow subgroup is isomorphic to $\mathbb{Z}_{\ell^n} \times \mathbb{Z}_{\ell^r}$.

Using these techniques, powers of an small ℓ of the cardinal of an elliptic curve over fields $\mathbb{F}_p$ can be computed in a very efficient way. For instance, the curve with equation $y^2 + axy + by = x^3$ over $\mathbb{F}_p$, $p = 10^{60} + 3201$, with coefficients

$$a = 591251564930225630443142051952893016614929347898787063526161$$

$$b = 588863440918737889900112853721548168318591022984529521909 84$$

has 2-Sylow and 3-Sylow groups isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$ and $\mathbb{Z}_{3^{11}} \times \mathbb{Z}_3$, respectively (these computations can be performed in less than a second using MAGMA [45]).

5.2 Elliptic curve generation by means of volcanoes of isogenies

Given an elliptic curve E over $\mathbb{F}_p$, all elliptic curves isomorphic to E have the same cardinal and group structure as $E(\mathbb{F}_p)$. However, different elliptic curves with the same cardinal are not necessarily isomorphic. As a matter of fact, all curves *isogenous* to E (see [16, 73]) have this property. So it is interesting to generate elliptic curves that are isogenous to a cryptographically useful elliptic curve. The goal is to provide as many good curves as possible without changing the arithmetic of the base field $\mathbb{F}_p$.

The set of all elliptic curves up to isomorphism with a given cardinal forms a complete directed graph. The vertices of this graph are isomorphism classes of elliptic curves, and the arcs are isogenies between them. The restriction to isogenies of certain prime degrees ℓ forms a subgraph which is not necessarily connex. Each connex component is stratified into different levels, forming a so-called *volcano* structure [40] because of its special shape. More precisely, a volcano consists of a cycle or *crater*, from each of whose vertices hangs an $(\ell - 1)$-complete tree. All these trees are isomorphic. Kohel explored such a structure to determine the endomorphism ring of a given elliptic curve with known cardinal. An ℓ-volcano for $\ell = 3$ is shown in Figure 2.

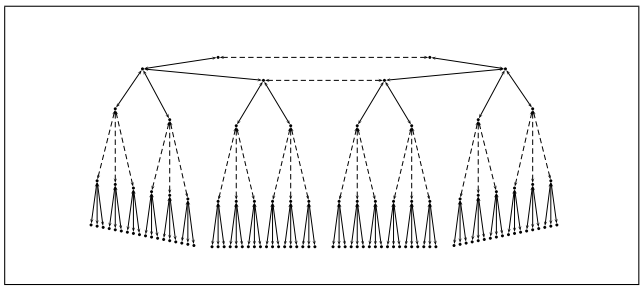

Figure 2. Volcano of 3-isogenies.

On the other hand, Fouquet-Morain [20] provide an algorithm to determine the height of a volcano. Their method consists of an exhaustive search over several paths on the volcano to detect the crater and the floor levels. In each step, they compute the roots of the ℓ-modular polynomial in order to obtain the j-invariant of the isogenous curves. In [56] the relationship between the levels of the volcano and the ℓ-Sylow subgroup structure of the curves is described. Using this relationship and

Vélu's formulae [75] (which allow explicit equations for isogenies to be obtained) it is possible to design an algorithm to compute, for a given elliptic curve E, the height and the length of the crater of its ℓ-volcanoes for $\ell = 2, 3$, and also to determine the list of curves isogenous to E (see [54, 56]). For instance, the volcano of 2-isogenies of the elliptic curve with Legendre equation $y^2 = x(x-1)(x-\lambda)$ with $\lambda = 4$ over $\mathbb{F}_p$, $p = 10^{100} + 1357$ has height 2 (and 3 levels) and the length of crater is 2. The whole volcano has 14 vertices, and among the 14 curves isogenous to E one finds for example the curve with parameter

$$\begin{aligned}\lambda =& 337520270738387966719808441910759004042\\ & 517694725911723994826495106127011135439 44\\ & 61131215697274948282\end{aligned}$$

Experimental results point out that the average height of these volcanoes is very small, while the length of their craters can be huge. For example the volcano of the curve $y^2 = x(x-1)(x-2017156814720162)$ over the field $\mathbb{F}_p$ with $p = 8010956020551503$ has a height of 1 and crater length of 74638817.

The algorithm can also be implemented for other small primes ℓ. In the same fashion, if one considers different values of ℓ for the same curve E, it is possible to cover all the connex components of whole ℓ-range of volcanoes (see [55]), and this increases the desired number of curves isogenous to E. This algorithm provides many more curves isogenous to a cryptographically suitable elliptic curve, hence their interest from a practical point of view follows. Furthermore, this procedure can be significantly improved by using paralellization techniques, as shown in [46].

Besides, it should also be mentioned that, although the cardinal is an invariant under isogeny, there might be other properties (such as group structure or magic number [25], for instance) that are not. Depending on these parameters, curves could be weaker. In particular, the Weil descent attack to the ECDLP exploits such a fact, embedding the group $E(\mathbb{K})$ in the divisor class group of hyperelliptic curves defined over a proper subfield of $\mathbb{K}$ given by the Weil restriction [21, 30]. Galbraith, Hess and Smart [24] suggest a procedure to find an isogenous curve where the Weil descent attack is effective, by means of a random walk over the volcanoes of isogenies.

6 Privacy and security in computationally restricted systems

During recent years, industry has been paying a lot of attention to the development of smart cards and RFID (Radio Frequency Identification) technologies, for use in many e-commerce and financial applications [64, 62]. In both cases, the computational capabilities of these devices are limited, so security mechanisms fitting such restrictions are needed.

Smart cards include an embedded microchip which can process some information, deal with some limited memory capacity, as well as execute some computational processes that are not too complex or costly. These cards are often used in identification mechanisms, implementing some cryptographic algorithms. Among the huge amount of applications, their use as credit cards, SIMs for mobile phones, access control cards, and authorization cards in pay-per-view systems should be mentioned.

On the other hand, an RFID mechanism is a last generation technology which provides an automatic method for identifying objects at distance, by using radio communications. RFID tags are attached to each object. These tags consists of a microchip and an antenna, which permit communication by means of a wireless channel. However, in the case of passive tags, they require no internal power source. There is also a wide range of applications of these systems, going from object control in production chains, product labelling in department stores (allowing automatic stock control as well as instantaneous computation of the shopping cart cost), inclusion in electronic passports, and there are even some proposals suggesting their use in banknotes, such as controlling false banknotes or tracking them in illegal transactions.

In both scenarios, secure protocols are required to guarantee the correct behavior of the systems [65, 14]. Hence, the cryptographic algorithms need to fit the features of these environments, such as computational restrictions, reduced memory capacity and bandwidth. Elliptic curve cryptography turns out to be a good alternative to conventional cryptography, since the usage of smaller fields can provide cryptographic solutions which fit better these restrictions [3, 42, 80].

6.1 ECC on Smart Cards

Features of elliptic curve cryptography make them suitable for implementation on memory constraint devices such as smart cards. Nevertheless, the implementation must be done carefully, on the one hand to decrease the cost of the operations and on the other hand to avoid possible attacks.

Concerning the operation $k \cdot P$ over an elliptic curve, remember that it can be reduced to doubling and adding points, by using the binary method. These addition formulae (see (2)) need one inversion over the base field $\mathbb{F}_q$, which is more expensive than multiplication. So, for implementations on smart cards, it is usual to transform affine coordinates (x, y) into other coordinates where inversion is not required, as projective coordinates or Jacobian coordinates. In Jacobian coordinates, the elliptic curve is given by an equation $y^2 = x^3 + axz^4 + bz^6$, while points with coordinates $[x, y, z]$ and $[r^2x, r^3y, rz]$, $r \in \mathbb{F}_q^*$, correspond to the same point. Then the coordinates of $P+Q = [x_3, y_3, z_3]$ in terms of the coordinates of $P = [x_1, y_1, z_1]$ and $Q = [x_2, y_2, z_2]$ are given as follows:

- If $P = Q$, take $S = 4x_1y_1^2$, $M = 3x_1^2 + az_1^4$ and $T = -2S + M^2$. Then
$$x_3 = T,\ y_3 = -8y_1^4 + M(S - T),\ z_3 = 2y_1z_1.$$
- If $P \neq Q$, consider $U_1 = x_1z_2^2$, $U_2 = x_2z_1^2$, $S_1 = y_1z_2^3$, $S_2 = y_2z_1^3$, $H = U_2 - U_1$ and $R = S_2 - S_1$. Then
$$\begin{aligned} x_3 &= -H^3 - 2U_1H^2 + R^2,\\ y_3 &= -S_1H^3 + R(U_1H^2 - x_3),\\ z_3 &= z_1z_2H. \end{aligned}$$

Indeed, computation of inverses is avoided so that fast implementation on hardware devices can be optimized.

The Side Channel Attacks (SCA) on ECC over smart cards [7] are based on obtaining information from the behavior of the power consumption of these devices. Analyzing such patterns, the differences between the doubling and adding operation can be detected. Hence, an attacker observing the performance of a card computing $d \cdot P$ using the binary method, can easily manage to get the bits of the secret key, $d = (d_{n-1} \dots d_1 d_0)_2$. There are several approaches to avoid this *simple power analysis* attack, such as the Montgomery-type method, which forces the computation of both the doubling and the adding for each d_i. Nevertheless, the so called *differential power analysis*, can still be resistant to these methods by analyzing many power consumptions with statistical tools. There are also several countermeasures to prevent this attack, which are based on randomization methods, such as randomization of Jacobian coordinates.

A new attack [34], when the curve have points $(x, 0)$ or $(0, y)$, is the Goubin's power analysis attack. In this case, these points cannot be randomized in Jacobian coordinates either. Besides, this attack has been extended to the points corresponding to the zero values ZVP [1] of $3x^2 + a = 0$, $x^2 - a = 0$ and $x^2 + a = 0$, which appear in the auxiliary expressions of the adding formulae, including the Montgomery one. A countermeasure proposed to avoid this attack is the usage of isogenies. Indeed, an isogenous curve which has neither $(0, y)$ nor ZVP can be considered. Hence the computations can be made on this curve but then, using the isogeny equations, the resulting point will be given in the original curve.

7 Recent developments

In this section we sketch some recent research on the cooperative relationship between cryptography and algebraic curves.

There are some computationally interesting problems related to DLP. The Decisional Diffie-Hellman Problem DDHP, for instance, is being able to distinguish between the distributions $(P, a \cdot P, b \cdot P, ab \cdot P)$ and $(P, a \cdot P, b \cdot P, c \cdot P)$ where a, b, c are random in $\mathbb{Z}_p$ and P is an element of a suitable cyclic group of large prime order, typically a point of an elliptic curve.

Another problem closely related to DLP is the Computational Diffie-Hellman Problem CDHP, which consists of the actual computation of the element $ab \cdot P$ from $P, a \cdot P$ and $b \cdot P$. Note that an algorithm to solve DLP solves both DDHP and CDHP, so these matters only make sense in case DLP has no known efficient solution.

The rich theory of algebraic curves happens to provide useful tools to deal with such problems and define new challenges. For instance, in the case of elliptic curves there exists a bilinear, non-degenerate pairing

$$e_\ell(\cdot, \cdot) : E(\mathbb{F}_p)[\ell] \times E(\mathbb{F}_p)[\ell] \to \mathbb{F}_{p^k}^*$$

where ℓ is prime to p and k is the smallest number such that $\ell \mid p^k - 1$. For every pair P, Q of points in E, $e_\ell(P, Q)$ is an efficiently computable value of certain finite field. For some values of k, DDH becomes solvable in $E(\mathbb{F}_p)$ using non-degeneracy and bilinearity of $e_\ell(\cdot, \cdot)$. On the other hand, the existence of a pairing like $e_\ell(\cdot, \cdot)$ is useful to define the perhaps most common of all security assumptions today. This is the Bilinear Diffie-Hellman Assumption, namely that the computation of $e_\ell(P, P)^{abc}$ from $P, a \cdot P, b \cdot P, c \cdot P$ is hard.

One way to solve DDH in practice using pairings is by the means of distortion maps [76]. Roughly, these are group homomorphisms that enable the non-degeneracy property of $e_\ell(\cdot, \cdot)$ for all the pairs of elements in the group. Their existence is related to the shape of the endomorphism ring of the underlying elliptic curve, or the higher dimension abelian variety if this is the case [27, 26].

The Identity-Based Encryption Scheme by Boneh and Franklin [5] is a good example of how to exploit this extra structure. Their scheme is the first fully functional encryption scheme that avoids the need to obtain public key certificates to send messages, as the authentication step is transfered to become a matter between the receiver and a Certification Authority. We briefly sketch now how it works.

Protocol (Identity-Based Encryption Scheme)

- Step 1. The Certification Authority makes public the parameters of the scheme: two groups G_1, G_2, a pairing $e(\cdot, \cdot) : G_1 \times G_1 \to G_2$, a generator P of G_1 and $P_{pub} = s \cdot P$ for a secret *master key* $s \in [1, q-1]$.
- Step 2. For a string id of bits typically associated to the email address of the receiver, CA associates $Q_{id} \in G_1$ and sets the private key of the receiver $d_{id} = s \cdot Q_{id}$.
- Step 3. A sender encrypts a message M for the public key id computing Q_{id} and $g_{id}^r = e(Q_{id}, P_{pub})^r \in G_2$, for a random $r \in [1, q-1]$, and then transmitting the pair $C = (r \cdot P, M \oplus g_{id}^r)$.
- Step 4. The receiver is able to decrypt $C = (U, V)$ using his secret key d_{id} to compute $V \oplus e(d_{id}, U) = M$ because

$$\begin{aligned} e(d_{id}, U) &= e(s \cdot Q_{id}, r \cdot P) = e(Q_{id}, P)^{sr} \\ &= e(Q_{id}, P_{pub})^r = g_{id}^r. \end{aligned}$$

8 Further cryptographic applications

Elliptic curves also play a remarkable role in other subjects directly related to cryptography and cryptanalysis, for example primality tests or factorization algorithms [10]. Primality tests are a fundamental tool in the setup of public key cryptosystems like RSA and ElGamal. Although probabilistic tests are often used to detect potentially composite numbers, it is convenient to use deterministic tests to grant and certify the primality of a given number. For instance, in ElGamal schemes the prime p determines the base field and consequently the modular arithmetic to be used. One of the best known primality tests based on elliptic curves is the Goldwasser-Kilian test [31]. Their method is the elliptic curve version of a result by Pocklington-Lehmer for $\mathbb{Z}_N^*$, but they work with the group $E(\mathbb{Z}_N)$ instead (here N is the integer to certify). While the group $\mathbb{Z}_N^*$ is of no use when

$N-1$ does not verify certain properties, the group $E(\mathbb{Z}_N)$ has the advantage that the equation of the elliptic curve can be modified until a cardinal with the required conditions is found. The main drawback for using elliptic curves is the computational cost of the group order and its factorization, as well as the determination of a point of large enough order. To avoid all these computations, Atkin and Morain [2] propose a primality test which relies on the construction of elliptic curves with prefixed cardinal and j-invariant using the theory of complex multiplication. The implementation of their test is very efficient, and they are able to prove primality for numbers of 100 digits.

Concerning the integer factorization problem, the properties of elliptic curves are also exploited in the design of new algorithms. Lenstra's algorithm [43] for instance is inspired in Pollard's $p-1$ method (which tries to find a factor p of an integer N that is the product of $p-1$ small primes), but as in the case of primality tests, uses the groups $E(\mathbb{Z}_N)$ instead of $\mathbb{Z}_N^*$. The point manipulation in Lenstra's algorithm is via projective coordinates, and with the multiples $k \cdot P = [x, y, z]$ of a point P of $E(\mathbb{Z}_N)$ it is possible to find a factor p of N from $\gcd(z, N)$ when varying P and $E/\mathbb{Z}_N$.

Modern factorization algorithms like Lenstra's or the Number Field Sieve were successful breaking large RSA moduli. To encourage the research on these topics, as well as to test their performance, RSA Laboratories have been posting several challenges [68] consisting of a set of integers to be factored. Hence, since 1991 several challenges have been broken, ranging from 100 to 200 digit-length integers. The last one was the so-called RSA-200 Challenge, which was factored in 2005. There are still lots of challenges to defeat, the largest one being around 600 digit-length. Similarly, Certicom also issued some challenges [9] to solve the ECDLP in a cyclic subgroup of an elliptic curve. They are named ECCp-d and ECC2-d to distinguish whether the base field is $\mathbb{F}_p$ or $\mathbb{F}_{2^m}$, and where d is the bit-length of the order of the cyclic subgroup. Moreover, when using Koblitz curves over $\mathbb{F}_{2^m}$, the challenges are called ECC2K-d. To date, the most recently solved challenges are: ECC2K-108 was solved using a distributed version of Pollard's ρ in year 2000, ECCp-109 fell in 2002 and ECC2-109 fell in year 2004, with help of 2600 computers working 17 months. The next unbroken one is ECCp-131, with an estimated workload of around 2.3^{10} machine days. This challenge is defined by the following parameters (in hexadecimal notation):

$$
\begin{aligned}
p &= 04\ 8E1D43F2\ 93469E33\ 194C4318\ 6B3ABC0B \\
a &= 04\ 1CB121CE\ 2B31F608\ A76FC8F2\ 3D73CB66 \\
b &= 02\ F74F717E\ 8DEC9099\ 1E5EA9B2\ FF03DA58 \\
n &= 04\ 8E1D43F2\ 93469E31\ 7F7ED728\ F6B8E6F1 \\
x_P &= \ 03\ DF84A96B\ 5688EF57\ 4FA91A32\ E197198A \\
y_P &= 01\ 47211619\ 17A44FB7\ B4626F36\ F0942E71 \\
x_Q &= 03\ AA6F004F\ C62E2DA1\ ED0BFB62\ C3FFB568 \\
y_Q &= 00\ 9C21C284\ BA8A445B\ B2701BF5\ 5E3A67ED
\end{aligned}
$$

where n is the order of the point $P = (x_P, y_P)$ on the curve $y^2 = x^3 + ax + b$ over $\mathbb{F}_p$. The goal is to compute k such that $k \cdot P = (x_Q, y_Q)$.

Interestingly enough, all these advances in cryptanalytic techniques and results foster research in the opposite direction, that of the design of even more resistant and secure cryptographic protocols: proposals of new methods, exploration of the suitability of other groups, such as the Jacobian of a hyperelliptic curve or other abelian varieties [4, 11], the definition of new computationally hard mathematical problems,...

References

[1] T. Akishita and T. Takagi, Zero-value point attacks on elliptic curve cryptosystem. *Information Security, ISC 2003*, LNCS 2851, 218–233, 2003.

[2] A. O. L. Atkin and F. Morain, Elliptic curves and primality proving. *Mathematics of computation*, 61, no. 203, 1993, 29–68.

[3] L. Batina, J. Guajardo, T. Kerins, N. Mentens and P. Tuyls, I. Verbauwhede. An Elliptic Curve Processor Suitable For RFID-Tags, *1st Benelux Workshop on Information and System Security, WISSec2006*, 2006.

[4] P. Bayer *et al.* Arithmetical problems in number fields, abelian varieties and modular forms. *Contributions to Science*, 1 (2): 125–145, 1999.

[5] D. Boneh and M. Franklin, Identity-Based Encryption from the Weil Pairing. *Crypto 2001*, LNCS 2139, Springer-Verlag (2001), 213–229.

[6] I. Blake, G. Seroussi and N. Smart, *Elliptic Curves in Cryptography*. London Mathematical Society, LNS 265, Cambridge University Press, 2000.

[7] E. Brier and M. Joye, Weierstrass Elliptic Curves and Side-Channel Attacks. *Public Key Cryptography*, LNCS 2274, 335–345, 2002.

[8] J. W. S. Cassels, Diophantine equations with special reference to elliptic curves. *Journal of the London Mathematical Society*, 41, 1966, 193–291.

[9] Certicom Corp. *Certicom ECC Challenge*. Available from http://www.certicom.com/download/aid-111/cert_ecc_challenge.pdf

[10] H. Cohen, *A Course in Computational Algebraic Number Theory*, GTM, no. 138, Springer-Verlag, Berlin, 1993.

[11] H. Cohen and G. Frey, *Handbook of elliptic and hyperelliptic curve cryptography*. Chapman & Hall/CRC, 2006.

[12] J. E. Cremona, Subject: amusing fact about elliptic curves over finite fields, August 2004. nmbrthr@listerv.nodak.edu.

[13] J. Daemen and V. Rijmen. *The Design of Rijndael*, Springer-Verlag, 2002.

[14] I. Damgard and M. Ostegaard, RFID *Security: Tradeoffs between Security and efficiency*, IACR eprint, july 2006. Available from http://eprint.iacr.org/2006/234.

[15] N. Demytko, A new elliptic curve based analogue of RSA. *Advances in Cryptology-EUROCRYPT'93*, LNCS 765, 1993, 40–49.

[16] M. Deuring, *Die Typen der Multiplikatorenringe elliptischer Funktionenkörper*, Abh. Math. Sem. Hansischen Univ. 14, 1941, 197–272.

[17] W. Diffie and M. E. Hellman, New directions in Cryptography. *IEEE Transactions on Information Theory*, vol. IT-22, 1976, 644–654.

[18] J. Domingo and J. Herrera, *Criptografia per als serveis telemàtics i el comerç electrònic*. Edicions Universitat Oberta Catalunya, 1999.

[19] T. ElGamal, A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Trans. Inform. Theory*, 31, no. 4, 1985, 469–472.

[20] M. Fouquet and F. Morain, Isogeny Volcanoes and the SEA Algorithm. *Proc. ANTS-V*, LNCS 2369, Springer 2002, 276–291.

[21] G. Frey, Applications of arithmetical geometry to cryptographic constructions. *Proc. V International Conference on Finite Fields and Applications*, Springer, 2001, 128–161.

[22] A. Fúster, D. de la Guía, L. Hernández, F. Montoya and J. Muñoz, *Técnicas criptográficas de protección de datos*. Ra-Ma, 2004.

[23] S. Galbraith, Elliptic curve Paillier schemes. *J. of Cryptology*, 15, no. 2, 2002, 129–138.

[24] S. Galbraith, F. Hess and N. Smart, Extending the GHS Weil descent attack. *Advances in Cryptology-EUROCRYPT'02*, LNCS 2332, 2002, 29–44.

[25] S. Galbraith and A. Menezes, Algebraic curves and cryptography. *Finite fields and their applications*, 11, 2005, 544-577.

[26] S. Galbraith, J. Pujolàs, C. Ritzenthaler and B. Smith, Distortion maps for genus two curves. *Journal of Mathematical Cryptology*, 2007.

[27] S. Galbraith and V. Rotger, Easy decision Diffie-Hellman groups. *LMS J. Comput. Math.*, 7, 2004, 201–218.

[28] D. Galindo, S. Martín, P. Morillo and J. Villar, A practical public key cryptosystem from Paillier and Rabin schemes. *PKC 2003*, LNCS 2567, 2003, 279–291.

[29] D. Galindo, S. Martín, T. Takagi and J. Villar, A provably secure elliptic curve scheme with fast encryption. *Progress in Cryptology-INDOCRYPT'04*, LNCS 3348, 2004, 245–259.

[30] P. Gaudry, F. Hess and N. Smart, Constructive and destructive facets if Weil descent on elliptic curves. *J. of Cryptology*, 15, 2002, 19–46.

[31] S. Goldwasser and J. Kilian, Almost all primes can be quickly certified. *Proc. 18th STOC*, 1986, 316–329.

[32] S. Goldwasser and S. Micali, Probabilistic encryption. *J. Computer and System Sciences*, 28, no. 2, 1984, 270–299.

[33] J. L. Gómez Pardo, Criptografía y curvas elípticas. *La Gaceta de la RSM* 5, no. 3, 2002, 738–77.

[34] L. Goubin, A refined power-analysis attack on elliptic curve cryptosystems. *Public Key Cryptography-PKC 2003*, LNCS 2567, 199–211, 2003.

[35] D. Hankerson, A. Menezes and S. Vanstone, *Guide to Elliptic Curve Cryptography*, Springer, 2003.

[36] H. Hasse. Zur Theorie der abstrakten elliptischen Funktionenkorper. III. Die Struktur des Meromorphismenrings; die Riemannsche Vermutung. *J. Reine Angew. Math.* 175, 1936, 193–208.

[37] M. Joye and J. Quisquater, Reducing the elliptic curve cryptosystem of Meyer-Müller to the cryptosystem of Rabin-Williams. *Designs, codes and Cryptography*, vol. 41, no. 1, 1998, 53–56.

[38] N. Koblitz, Elliptic Curve Cryptosystems. *Mathematics of Computation*, no. 177, 1987, 203–209.

[39] N. Koblitz, *Algebraic aspects of cryptography*. Springer-Verlag, 1998.

[40] D. Kohel, *Endomorphism rings of elliptic curves over finite fields*. PhD Thesis, University of California, Berkeley, 1996.

[41] K. Koyama, U. Maurer, T. Okamoto and S. Vanstone, New public-key schemes based on elliptic curves over $\mathbb{Z}_n$. *Adv. Cryptology-CRYPTO'91*, LNCS 576, 1991, 252–263.

[42] T. Lange, Arithmetic on Binary Genus 2 Curves Suitable for Small Devices, *Workshop on RFID and Lightweight Crypto*. Proceedings, 67–77, 2005.

[43] H. W. Lenstra, Factoring integers with elliptic curves. *Ann. Math.*, 126, 1987, 649–673.

[44] R. Lercier, Subject: Elliptic curve point counting: 100002 bits, nmbrthr@listerv.nodak.edu, December 2002.

[45] MAGMA GROUP, *Handbook of Magma functions*, J. Canon and W. Bosma, eds. Available from http://magma.maths.usyd.edu.au/.

[46] S. Martínez, R. Tomàs, C. Roig, M. Valls and R. Moreno, Parallel calculation of volcanoes for cryptographic uses. *7th Workshop on Parallel and Distributed Scientific and Engineering Computing, PDSEC-IPDPS'06*, IEEE Computer Society Press, 2006.

[47] A. Menezes. *Elliptic Curves Public Key Cryptography*, Kluwer, 1993.

[48] A. Menezes, T. Okamoto and S. Vanstone, Reducing elliptic curve logarithms to logarithms in a finite field. *IEEE Transactions on Information Theory*, 39, 1993, 1639–1646.

[49] A. Menezes, P. van Oorschot and S. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1997.

[50] B. Meyer and V. Müller, A public key cryptosystem based on elliptic curves over $\mathbb{Z}_n$ equivalent to factoring. *Advances in Cryptology-EUROCRYPT'96*, LNCS 1070, 1996, 49–59.

[51] V. Miller, Uses of elliptic curves in cryptography. *Advances in Cryptology-CRYPTO'85*, LNCS 218, 1986, 417–426.

[52] J. Miret, R. Moreno and A. Rio, Generalization of Vélu's formulae for isogenies between elliptic curves. *Publicacions Matemàtiques*, vol. extra, 2007, 147-163.

[53] J. Miret, R. Moreno, A. Rio and M. Valls, Determining the 2-Sylow subgroup of an elliptic curve over a finite field. *Mathematics of computation*, 74, no. 249, 2005, 411–427.

[54] J. Miret, R. Moreno, D. Sadornil, J. Tena and M. Valls, An algorithm to compute volcanoes of 2-isogenies of elliptic curves over finite fields. *Applied Mathematics and Computations*, Vol 176 no. 2 pp. 739–750, 2006.

[55] J. Miret, D. Sadornil, J. Tena, R. Tomàs and M. Valls, Isogeny cordillera algorithm to obtain cryptographically good elliptic curves. *Fifth Australasian Information Security Workshop*, ACSW Frontiers 68,127–132, 2007.

[56] J. Miret, D. Sadornil, J. Tena, R. Tomàs and M. Valls, Volcanoes of ℓ-isogenies of elliptic curves over finite fields: the case $\ell = 3$. *Publicacions Matemàtiques*, vol. extra, 2007, 165–180.

[57] R. Moreno, *Subgrupos de Sylow de las curvas elípticas definidas sobre cuerpos finitos*. PhD Thesis, Universitat Politècnica de Catalunya, 2005.

[58] C. Munuera and J. Tena, *Codificación de la Información*. Publicaciones de la Universidad de Valladolid, 1997.

[59] NSA Suite B Cryptography, http://www.nsa.gov/ia/industry/crypto_suite_b.cfm.

[60] NIST: National Institute of Standards and Technology. *Digital Signature Standard, FIPS PUB 186-2*, Enero 2000.

[61] P. Paillier, Public key cryptosystems based on composite degree residuosity classes. *Advances in Cryptology-EUROCRYPT'99*, LNCS 1592, 1999, 223–238.

[62] P. Peris-López, J. C. Hernández-Castro, J. Estevez-Tapiador and A. Ribagorda, RFID Systems: A Survey on Security Threats and Proposed Solutions. *International Conference on Personal Wireless Communications* PWC'06, 2006.

[63] S. Pohlig and M. Hellman, An improved algorithm for computing logarithms over GF(p) and its cryptographic significance. *IEEE Transactions on Information Theory*, vol. IT-24, 1978, 106–110.

[64] W. Rankl, W. Effing and W. Rankl, *Smart Card Handbook*. John Wiley & Sons, 2004.

[65] M. Rieback, B. Crispo and A. Tanenbaum, The Evolution of RFID Security. *IEEE Pervasive Computing*, 5(1), 2006, 62–69.

[66] A. Rio, *Criptografía y Seguridad en Bases de Datos*. E. Fernández-Medina, M. Piattini, M. A. Serrano (Eds). Fundación dInTel, Serie Monografías y P. 6, 2001, 326–345.

[67] R. Rivest, A. Shamir and L. Adleman, A method for obtaining digital signatures and PKC. *Communications of the ACM*. Vol. 21 (2), 1978, 120–128.

[68] RSA Laboratories, *The RSA Factoring Challenge*. Available from http://www.rsa.com/rsalabs/node.asp?id=2092.

[69] H. G. Rück, A note on elliptic curves over finite fields. *Mathematics of Computation*, 49(179), 1987, 301–304.

[70] J. Satoh, The canonical lift of an ordinary elliptic curve over a finite field and its point counting. *J. Ramanujan Math. Soc.* 15:247–270, 2000.

[71] R. Schoof, Elliptic curves over finite fields and the computation of square roots $\mod p$. *Mathematics of computation*, 44, no. 170, 1985, 483–494.

[72] R. Schoof, Nonsingular plane cubic curves over finite field. *Journal of Combinatorial Theory. Series A*, 46 (2), 183–211, 1987.

[73] J. H. Silverman, *The Arithmetic of Elliptic Curves*. GTM no. 106, Springer, 1986.

[74] J. H. Silverman and J. Suzuki, Elliptic curve discrete logarithms and the index calculus. *Advances in Cryptology-ASIACRYPT'98*, LNCS 1514, 1998, 110–125.

[75] J. Vélu, Isogénies entre courbes elliptiques. *C. R. de l'Académie des Sciences de Paris*, Série A, vol. 273, Académie des Sciences de Paris, 238–241, 1971.

[76] E. Verheul, Evidence that XTR is more secure than supersingular elliptic curve cryptosystems. *J. of Cryptology*, 17, 2004, 277–296.

[77] J. F. Voloch, A note on elliptic curves over finite fields. *Bulletin de la Société Mathématique de France*, 116, 1988, 455–458.

[78] E. Waterhouse, Abelian varieties over finite fields. *Annales scientifiques de l'École Normale Supérieure*, 4(2), 1969, 521–560.

[79] H. C. Williams, A modification of the RSA public-key encryption procedure. *IEEE Transactions on Information Theory*, IT-26, no. 6, 1980, 726–729.

[80] J. Wolkerstorfer, Is elliptic-Curve Cryptography suitable to Secure RFID Tags? *Workshop on RFID and Lightweight Crypto*. Proceedings, 78–91, 2005.

About the authors

The authors carry out their research activities in the Cryptography and Graphs Group in Universitat de Lleida*. They owe their formation to other catalan universities, such as* Universitat de Barcelona*,* Universitat Autònoma de Barcelona *and* Universitat Politècnica de Catalunya*, where they developed PhD's in related areas like Algebraic Geometry, Graph Theory, Number Theory and Computational Cryptography.*

Today, the members working in Cryptography are: J. Miret, R. Moreno, J. Pujolàs and M. Valls, and those working in Graph Theory are J. Conde, J. Gimbert and N. López. Currently there are several pre-doctoral students undertaking their thesis in both areas.

The research interests of the authors concern mainly the following topics: elliptic and hyperelliptic curve cryptography, algorithmic and computational problems of such curves over finite fields, and cryptographic protocols for computationally limited devices like smart cards and RFID tokens. Their work in these areas has been supported by several national grants, currently under MTM2007-66842-C02-02.